

ABSTRACT

A manager or an issuer issues a participation certificate, for an ordinary user who will newly join a group formed on a network made up of specified users, on which the manager or issuer creates
5 a digital signature by the use of a private key of the group. Members belonging to the group authenticate one another as belonging to the same group and as authorized members of the group, on the basis of their respective participation certificates.